CYBER STABILITY CONFERENCE

TOWARDS A MORE SECURE CYBERSPACE

2021 Conference Report

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. The 2021 Cyber Stability Conference (CS2021) was supported by the generous contributions of UNIDIR's Security and Technology Programme core donors: Germany, the Netherlands, Norway, Switzerland, and Microsoft. In addition, this year's conference was also supported by the Russian Federation.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

THE AUTHOR

Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and IMT School for Advanced Studies, Italy.

TABLE OF CONTENTS

1. INTRODUCTION

▲ UNIDIR Director Dr. Robin Geiss opening the Cyber Stability Conference 2021

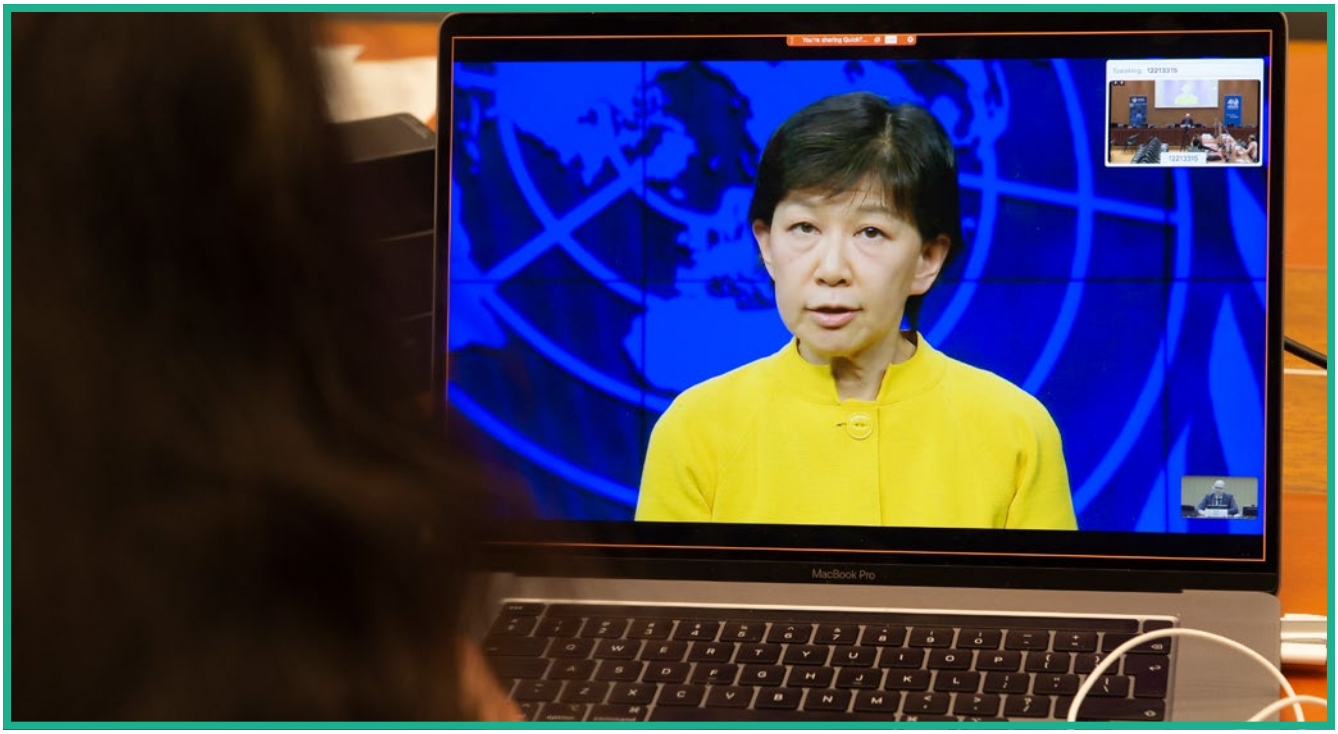
In the digital age, information and communications technology (ICT) underpins our core societal functions, and the reliance on this technology has grown further in the context of the COVID-19 pandemic. In 2021, which marked the second year of the pandemic, the two intergovernmental processes at the United Nations namely the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE) and the Open-Ended Working Group in the Field of Information and Telecommunications in the Context of International Security (OEWG). Both processes successfully produced consensus reports that were subsequently submitted to the General Assembly.[1]

Noting this progress, the Under-Secretary-General and High Representative for Disarmament, Izumi Nakamitsu, affirmed in her opening remarks to the conference, "[w]ith the successful conclusion of two intergovernmental processes this year… multilateral efforts to ensure a safe, secure and peaceful ICT environment have reached a high point". Indeed, as she further explained, "it is also encouraging that the General Assembly has returned to a single consensus Resolution and inter-governmental process on cybersecurity".

In December 2021, the second OEWG held its first substantial session. This was the first of a long series of meetings that will continue until 2025. The long length of this OEWG should allow United Nations Member States and other stakeholders to carefully engage in discussions that will cover many of the aspects that remain to be further defined and clarified on the development of information and telecommunications in the context of international security. Its mandate includes, "to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour."[2]

1 United Nations General Assembly. 2021a. *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies*, UN document A/RES/76/19, 8 December 2021. https://undocs.org/A/RES/76/19

2 United Nations General Assembly. 2021b, *Developments in the field of information and telecommunications in the context of international security*, UN document A/RES/75/240, 4 January 2021. https://undocs.org/en/A/RES/75/240



▲ Ms. Izumi Nakamitsu, Under-Secretary-General and High Representative for Disarmament Affairs, delivering her opening remarks.

In view of the successful conclusion of the two multilateral cyber processes and the beginning of a new OEWG, the UNIDIR Cyber Stability Conference 2021 (CS21): Toward a More Secure Cyberspace convened representatives from government, industry and civil society to reflect on how we can build on past successes to advance the agenda for an open, secure, stable, accessible and peaceful ICT environment; on what has been discussed and agreed upon so far; and on what should be prioritized next.

2. KEY TAKEWAYS

▲ A conference participant reading through the CS21 agenda.

- There is general agreement that United Nations Member States should strengthen and build on the achievements of the past GGEs and the first OEWG.
- In the discussions moving forward, a technology-neutral approach should be maintained with a focus on the effects of the malicious use of technology rather than on the technology itself. In particular, given the growing reliance of our societies on digital technologies, there should be greater consideration of the impact and harm resulting from the misuse of ICT on humans.
- Member States should strengthen their commitment to norms of responsible State behaviour in cyberspace by clarifying how the norms could be operationalized and implemented. This is particularly important given the low level of trust in the international community concerning States' adherence to the agreed cyber norms.
- There is agreement among Member States that international law applies to cyberspace. However, there is a need for greater clarity on Member State's views on how international law applies to cyberspace. More transparency in this regard would help foster a common understanding of the application of international law in cyberspace, avoid misunderstandings, and increase predictability and stability in the ICT environment.
- Sharing national positions on how to increase stability and predictability in cyberspace could be a favourable confidence-building measure. The UNIDIR Cyber Policy Portal is a valuable tool in this regard.
- Mutual trust is also key for capacity-building efforts as there are several cases where the recipient State does not have the capacity or the technical tools to verify the technology offered by the donors.
- There is a growing need to formally and systematically engage industry and civil society in the multilateral cyber processes, which has so far been limited to organizations accredited by the Economic and Social Council. New ways to engage with these non-State stakeholders could be explored.

3. SUMMARY OF THE DISCUSSION

CS21 was structured around the thematic pillars of the discussions under the GGE and the OEWG, including:

- Existing and potential threats
- Rules, norms and principles for responsible State behaviour
- International law
- Confidence-building measures
- Capacity building

The conference included a dedicated panel on each theme that explored what has been agreed so far and addressed how the agenda on each of these key areas can be advanced.

3.1 EXISTING AND POTENTIAL THREATS

Both the GGE and the OEWG processes agreed on the characterization of the threat environment. In this regard, Member States have expressed growing concerns about technologies that could be used to undermine international peace and security. Over the past 20 years, there has been rapid and considerable advancement in ICT, which is now embedded in every aspect of society. While this has transformative benefits, it also provides new methods and opens new pathways for misuse. Member States have also acknowledged that threat assessments vary by region and by State and that what constitutes a threat varies depending on the sector, demographics and ICT capacities.

Yet, both the GGE and the OEWG processes have been less focused on identifying specific existing and potential threats, such as the exploitation of vulnerabilities for malicious purposes. Moreover, several areas of concern that were discussed during the first OEWG were eventually not included in its substantive report. These include the stockpiling of vulnerabilities, the integrity of the ICT supply chain, data security, and mis- and disinformation.

In the light of rapid technological developments – such as increased automation and autonomy in ICT operations, quantum computing, expansion of big data, and increased digitization of personal data – Member States should strengthen their oversight of existing and potential threats that such developments could pose. Nevertheless, it will be challenging for time-bound multilateral discussions in the framework of the second OEWG to identify, comprehend and address the range of threat implications of new technological developments and trends to peace, security and stability in cyberspace. For example, quantum computing could outpace encryption, and cloud computing may become obsolete in the near future. It may therefore be prudent for the Member States to maintain a technology-neutral approach and focus more on regulation of the potential effects of the malicious use of technology rather than regulating the technology itself.

▲ Head of UNIDIR's Security and Technology Programme, Dr. Giacomo Persi Paoli, presenting the speakers at the panel on Threats.

Furthermore, it is important for the Member States to focus on the human element of the threats, such as the effects and direct harm that the misuse of ICT can have on individual citizens. Indeed, regardless of the technology involved, the harm – such as the loss of personal data, access to digital services or control of devices – always affects people.

▲ UNIDIR researcher Dr. Andraz Kastelic moderating the panel from the conference room in Geneva.

3.2 RULES, NORMS AND PRINCIPLES FOR RESPONSIBLE STATE BEHAVIOUR

In December 2015, the General Assembly of the United Nations adopted resolution 70/237, which called upon the Member States to be guided by 11 non-binding norms proposed by the fourth GGE. In 2021 the final report of the sixth GGE added additional information on these norms, and it reaffirmed their value for responsible State behaviour in cyberspace. The 2021 substantive report of the first OEWG recognized and reaffirmed these 11 non-binding norms. It also acknowledged that voluntary and non-binding norms could contribute to peace and stability, and do not replace international law principles and obligations.

The 11 non-binding norms extensively cover a wide variety of issues regarding States' behaviour in cyberspace. For the time being, there has been no clear indication that they have left any gap in the normative framework. Yet, as also affirmed in the OEWG's substantive report, additional norms could be developed over time.[3] For example, Member States may decide to further elaborate on the issue of disclosure of vulnerabilities and add a norm that may clarify the scope and procedures for disclosure. Nevertheless, any further developments of new norms should not undermine the achievements obtained by the past GGEs and the first OEWG. The recognition of the 11 non-binding norms is an important milestone that must be preserved. The norms have been conceived to last over time, and they have maintained their relevance and suitability despite rapid progress in the ICT domain. Their sustainability relies on the fact that they are technologically neutral (e.g., they do not provide specific definitions for technological devices), and therefore they will not become obsolete because of continuing ICT developments.

3 United Nations General Assembly. 2021c. *Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/75/816, 18 March 2021. https://undocs.org/A/75/816, annex I, para. 7.

Besides the possibility of adding new norms to the existing set, Member States expressed the need to further understand how to operationalize and implement the 11 agreed non-binding norms. In this regard, sharing and disseminating good practices and experiences on implementation of the norms is key to further strengthening the agreement on and commitment to the norms; this is particularly important given the low level of trust in the international community concerning States' adherence to the agreed cyber norms.

Moreover, given the relevant role that the private sector plays in developing and operating the physical and digital infrastructure and services, it can also contribute to norm settings and development. However, so far, the inclusion of the private sector in the OEWG process has been limited. Indeed, only entities accredited to the Economic and Social Council could participate in the formal sessions of the OEWG. Therefore, new ways to engage with these actors should be considered. There are already existing proposals in this regard, such as a set of recommendations from the Cybersecurity Tech Accord on how to enhance inclusivity of the private sector in United Nations dialogues through a regular and structured engagement, which should be systemic instead of ad hoc.[4] The private sector can also engage through informal dialogue and discussion. The second OEWG foresees intersessional consultative meetings in which stakeholders can participate even if they are not accredited by the Economic and Social Council. For these actors, understanding the dynamics of the OEWG is thus essential for enhancing their involvement in the process.

4 Paris Call Working Group 3 on Advancing the United Nations Negotiations with a Strong Multistakeholder Approach. 2021. *Multistakeholder Participation at the UN: The Need for Greater Inclusivity in the UN Dialogues on Cybersecurity*, November. https://pariscall.international/assets/files/10-11-WG3-Multistakeholder-participation-at-the-UN-The-need-for-greater-inclusivity-in-the-UN-dialogues-on-cybersecurity.pdf

▲ An attendee checking the speakers of the International Law panel.

3.3 INTERNATIONAL LAW

Both the OEWG and GGE reports elaborate on international law. The substantive report of the first OEWG underlines that "States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment".[5] The final report of the GGE reaffirms the commitments of States to specific principles of the Charter of the United Nations, such as sovereign equality, the settlement of international disputes by peaceful means, refraining in their international relations from the threat or use of force, respect for human rights and fundamental freedoms, and non-intervention in the internal affairs of other States.[6]

Moreover, the 2021 GGE report provides a few additional elaborations on how international law applies to State conduct in cyberspace, providing limited guidance on the principles of internal sovereignty, international humanitarian law, the secondary obligations of State responsibility, including attribution, and the due diligence principle. The GGE report suggests that the Member States need to engage in further discussions and exchanges of views on how specific rules and principles of international law apply to the use of ICT by States. The need for additional work in this direction was also stressed by the OEWG Chair's summary report, which indicates that "further understanding was required on how international law applies to State use of ICTs".[7] Only through additional engagement by the Member States in clarifying this topic, would there be the possibility to deepen common understanding, avoid misunderstandings, and increase predictability and stability in the ICT domain.

5 United Nations General Assembly (2021c, annex I, para. 34).
6 United Nations General Assembly. 2021d. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN document A/76/135, 14 July 2021. https://undocs.org/A/76/135
7 United Nations General Assembly (2021c, annex II, para. 10).

In this regard, the second OEWG could represent an essential opportunity for the Member States to elaborate further on this topic. While addressing and clarifying how international law applies to ICT, Member States could also assess whether gaps exist in current international law. Yet, in providing additional understanding of how international law applies to cyberspace or in addressing possible gaps, the Member States should build on what has already been agreed and achieved in both the GGE and OEWG processes.

Multi-stakeholder involvement also remains key concerning the better understanding of the impact of international law on a wide variety of non-State actors, which have a relevant role in the ICT environment. Given that some Member States found that the first OEWG posed strict limitations on stakeholders' engagement, new ways and opportunities to grant multi-stakeholder access to the OEWG process should be explored.

▲ A framing of UNIDIR researcher Dr. Samuele Dominioni moderating the panel on CBMs.

3.4 CONFIDENCE-BUILDING MEASURES

The concept of a confidence-building measure (CBM) is well-established, born during the Cold War period, and it is finding a new application in the field of ICT. CBMs in the ICT domain were first referred to by the 2010 report of the GGE, and since then they have been further defined and elaborated in all the agreed reports. Both the GGE and the OEWG reports recognize that CBMs could prevent conflicts, avoid misunderstandings and reduce tensions. The CBM section of the 2021 GGE report clearly differentiates between cooperative measures (which include the establishment of points of contact and dialogue and consultations) and transparency measures (where it reiterates the need to exchange national views and practices). States acknowledged that practical CBMs had been recommended in previous GGE reports, underlining at the same time that CBMs remain voluntary and that regional and subregional organizations are vital to their development. Both reports acknowledge that the UNIDIR Cyber Policy Portal is a valuable tool in this regard.

There are some aspects of CBMs on which the second OEWG may further elaborate. For example, the Member States may address how to better engage in implementing transparency measures. Indeed, in the first OEWG, some Member States committed to sharing their views on how to increase stability and predictability in cyberspace and they published them in the compendium of statements to the final report. It would be propitious for more Member States to share their views. Countries that have not yet elaborated their positions may begin sharing other relevant documents, such as, for example, national strategies on cyberspace. The UNIDIR Cyber Policy Portal could be considered for this purpose.

The second OEWG has a very important role concerning CBMs, especially in engaging the stakeholder community in continuing the global dialogue on CBMs. In fact, building confidence requires constant and enduring engagement of all stakeholders. These include the private sector, which should be further engaged to foster transparency in information sharing and cooperation. Key to the purpose of dialogue is the clarification of a shared understanding of concepts and terminology.[8] In the light of this, and given the different conceptualization of some ICT terms, it has been noted that regional contexts are better suited to building a common understanding of terminology and concepts.

Regional settings and organizations remain vital for the further development and implementation of CBMs. Indeed, the regional level is better suited for these purposes because progress there tends to be faster, as it is often easier to build confidence within an established relationship. Regional organizations, such as the Organization for Security and Co-operation in Europe (OSCE), also help to reduce the costs for the Member States to set up different bilateral CBMs across the region and beyond. Moreover, in some cases, regional organizations include States that may not have a well-established bilateral relationship.

8 United Nations General Assembly (2021c, annex II, para. 29).

▲ UNIDIR researcher Ms. Molihei Makumane moderating virtually the panel on Capacity Building.

3.5 CAPACITY-BUILDING

Capacity building is a cross-cutting issue and an enabler to increase stability and security in the ICT environment. The substantive report of the first OEWG elaborates extensively on capacity building, laying out the guiding principles for States in the implementation of capacity-building programmes. These principles cover process and purpose, partnerships, and people.[9] The OEWG's substantive report also affirms that "capacity-building is a reciprocal endeavour, a so-called 'two-way street', in which participants learn from each other and where all sides benefit from the general improvement to global ICT security. The value of South–South, South–North, triangular, and regionally focused cooperation was also recalled."[10]

Despite the relevant developments in the field of capacity building, some key issues require further consideration from the international community and, in particular, by the second OEWG. There is a need to further understand how to operationalize the OEWG approach to capacity building by appraising how current trends in the development cooperation sector, including capacity-building programmes, reflect the recommendation of the first OEWG's substantive report.

Indeed, lately, new approaches have emerged among practitioners that provide alternative solutions to the usual methods for capacity building. For example, a long-standing practice for project implementation consists of experts going to the recipient State for a short period, with limited engagement with the local stakeholders. An emerging trend is to deploy experts in the recipient State for extended periods, thereby providing a more permanent presence. With this approach,

9 United Nations General Assembly (2021c, annex II, para. 29).
10 United Nations General Assembly (2021, annex I, para. 57).

experts engage more with the local stakeholders, helping to build trust and transferring knowledge and expertise. Another emerging trend concerns the regionalization of capacity-building programmes. In this approach, donors establish regional centres to better tailor programmes and projects that rely on local capacity and informed expertise, which are crucial to meeting local needs. This trend, which has a very positive outlook, could be considered and supported by the OEWG process.

Beyond current trends, there are also unresolved issues in capacity-building efforts that the OEWG could address. Again, trust is a challenging question, which significantly hampers States' relationships in the ICT environment. The low level of trust in this domain can have detrimental effects on capacity building. Indeed, trust is critical in this sector because capacity-building programmes often imply technology transfer. Given that the recipient State often lacks the capacity or the technical tools to verify the technology offered, a trustful relationship between donors and recipients is thus vital.

The United Nations, and the OEWG, could further sustain capacity-building efforts in several ways. For example, the United Nations can provide a matchmaking platform by identifying needs and support between donors and recipient States, and promoting and fostering trust among stakeholders. Moreover, the United Nations could continue raising awareness concerning the importance of capacity building across world regions.

4. CONCLUSION AND THE WAY FORWARD

▲ In-person participants at the hybrid conference hosted online and in Geneva.

The positive conclusion of the two multilateral cyber processes, the sixth GGE and the first OEWG, came as a result of a long series of successes and failures since the inception of the multilateral process at the United Nations, back in 1998. These achievements are a positive indication that multilateralism is effective and that consensus is achievable, although such outcomes are largely dependent on the wider international security environment.

In December 2021, the General Assembly adopted a resolution that recognized the work of both the OEWG and the GGE and further called on Member States to be guided in their use of ICT by the reports of the GGE and the OEWG that concluded in 2021.[11] This resolution was co-sponsored by the Russian Federation and the United States of America, among others, and it has been considered as a positive step in support of the second OEWG.

Stemming from these developments, the second OEWG, which has already started its proceedings, could represent an opportunity to address some key issues that require further consideration by the international community. Of paramount importance is to better understand Member States' views on implementing the cyber norms and how international law applies to cyberspace. Sharing these standpoints is key to building trust, predictability and stability in the cyber domain, as well as to evaluating whether the current normative framework is sufficient to ensure an open, secure, stable, accessible and peaceful ICT environment.

The new OEWG could additionally work towards clarifying and building a shared understanding of key terms and concepts, which is vital for advancing discussions on central themes addressed by the OEWG. Moreover, given the growing critical role of non-state actors, including the private sector and civil society in the ICT domain, it is becoming increasingly necessary to formally and systematically engage with these stakeholders. In this regard, the OEWG could, in its work, explore new ways and opportunities for these non-State stakeholders to contribute to the process.

11 United Nations General Assembly (2021a).

2021 Conference Report

CYBER STABILITY CONFERENCE

TOWARDS A MORE SECURE CYBERSPACE

This report provides a short summary of the 2021 edition of UNIDIR's Cyber Stability Conference (CS2021) held in Geneva on 3 December 2021 The event focused on discussing the progress of the two multilateral United Nations (UN) processes on cyberspace, namely the Group of Governmental Experts on Advancing responsible State behaviors in cyberspace in the context of international security (GGE) and the Open-Ended Working Group in the Field of Information and Telecommunications in the Context of International Security (OEWG). The conference convened representatives from government, industry, and civil society to reflect on how we could build on past successes to advance the agenda for an open, secure, stable, accessible, and peaceful ICT environment.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH